CRD report

News from the LBNL Computational Research Division

January 2006

CRD's Chevassut Shares Expertise in Cryptography

Olivier Chevassut, who is the lead cryptographer for CRD, continues to build a reputation as an international expert on the theoretical and practical aspects of both cryptography and network security. In the first few months of 2006, Chevassut and several collaborators will have three conference papers and one journal article published.

Olivier Chevassut

As part of his work in designing and analyzing novel complex cryptographic technologies, Chevassut has served as the lead of a project entitled "Cryptographic Foundations for New Generation Distributed Systems," also known as CryptoGrid, to complete an analysis and design of the next generation Grid security infrastructure.

Here's a glance at his upcoming publications:

Along with co-authors Michel Abdalla, Emmanuel Bresson and David Pointcheval, Chevassut wrote "Provably Secure Password-Based Authentication in TLS." The paper will be published in the Proceedings of the ACM Symposium on InformAtion, Computer and Communications Security (ASIACCS'06), to be held March 21-24 in Taipei, Taiwan. The paper, which describes how to design an efficient, provably secure password-based authenticated key exchange mechanism specifically for the TLS (Transport Layer Security) protocol, is on line at <http://www.dsd.lbl.gov/Projects/OPKeyX/Publications/ASIACCS06/asiaccs06.html>.

A paper entitled "The Twist-Augmented

(continued on page 2)

CRD Report

CRD Report is published every other month, highlighting recent achievements by staff members in Berkeley Lab's Computational Research Division. Distributed via email and posted on the Web at http://crd.lbl.gov/DOEresources, CRD Report may be freely distributed. CRD Report is edited by Jon Bashor, JBashor@lbl.gov or 510-486-5849.

CRD's PyGlobus Tools Proving Popular

CRD's Distributed Systems Department (DSD), which has led the development of the de facto standard tools for developing Grid Services, applications and portals using the Python programming language, proved a popular draw at the LBNL booth at the SC05 conference in Seattle.

Python is a high-level interpreted language that supports a rapid application development cycle. Python's minimal syntax makes it an ideal language for use by non-computer scientists. It also easily supports binding together C/C++ and Fortran codes and exposing them through a thin Python interface. By enabling scientists to focus less on computer science details, our Python Grid tools allow scientists to focus on their science.

Keith Jackson led DSD's development of the Python Commodity Grid (CoG) Kit, or pyGlobus, to provide access to the original Globus Toolkit developed at Argonne National Lab and USC's Information Sciences Institute. The Python CoG Kit has been an important part of Grid development for a number of projects, including the DOE-funded Access Grid project and the NSF-funded Laser Interferometer Gravitational Wave Observatory (LIGO).

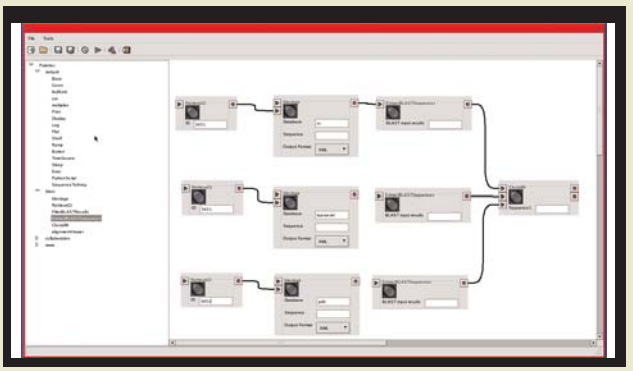
The Python CoG Kit provides a thin veneer of Python over the underlying Globus Toolkit C code. pyGlobus provides a simple, easy to use, object-oriented interface to Globus while still providing the full power and performance of the underlying C code.

The department also developed a Python implementation, called pyGridWare, of the next generation of Grid standards based on Web services, i.e., the Web Service Resource Framework (WSRF) and Web Service Notification (WS-N) specifications. In

(continued on page 2)

ViCE Helps Smooth Scientific Workflows

DSD's work in higher-level interfaces to the Grid has led to the development of a visual programming tool, ViCE, that is used to collaboratively develop and execute complex scientific workflows.



A typical ViCE workflow that shows a scientist using the BLAST search technology to search three protein sequence databases (nr, the main protein sequence database; topsecret, an example of proprietary data; and pdb, the Protein Structure Databank), then extracting the resulting sequences and aligning them using the ClustalW application.

Scientific projects today are frequently large collaborations among geographically and organizationally distributed teams. ViCE is designed to support scientists collaborating over a visual description of their workflow. A workflow is represented as a set of nodes and links. The nodes represent actions, such as querying a protein sequence database, and links represent the data transfer between nodes. By dragging and dropping a series of domain-specific nodes onto a palette, a scientist can construct a complete workflow.

The accompanying figure shows a typical visual workflow description from biology. The biologists are searching several protein sequence databases, looking for a likely match to a newly sequenced protein.

ViCE supports collaboration by allowing multiple groups to have the same view of the changing workflow description. They can use integrated chat tools to discuss the workflow. Future versions will support the collaborative editing of the visual workflow description.

Bailey Co-Organizes Math Course


David Bailey

David H. Bailey, the Chief Technologist of the Computational Research Division, co-organized a two-day course entitled "Experimental Mathematics in Action" at the annual joint meeting of the American Mathematical Society and the Mathematical Association of America. The meeting was held January 10-15 in San Antonio, Texas.

Approximately 80 people signed up for the course, which was organized in the spirit of the two recent books by Bailey and Jonathan Borwein, *Mathematics by Experiment: Plausible Reasoning in the 21st Century (2004) and Experimentation in Mathematics: Computational Paths to Discovery* (2004), the latter with Roland Girgensohn.

Although the texts served as a good primer for the course, the specific topic lectures in the course were primarily new material. Bailey gave two 90-minute lectures focusing on algorithms for experimental mathematics and on case studies of using high performance computing technology in mathematical research.

The goal of this course was to present a coherent variety of accessible examples of modern mathematics where intelligent computing plays a significant role and in doing so to highlight some of the key algorithms and to teach some of the key experimental approaches.

"The last twenty years have been witness to a fundamental shift in the way mathematics is practiced," according to the course abstract. "With the continued advance of computing power and accessibility, the view that 'real mathematicians don't compute' no longer has any traction for a newer generation of mathematicians who can readily take advantage of computer aided research, especially given the maturity of modern computational packages such as Maple, Mathematica and Matlab."

Bailey and the other four speakers in the course prepared written material to accompany the lectures and which will be published later this year as a book.

PyGlobus Tools Are Popular *(continued from page 1)*

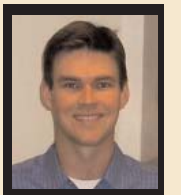
addition to building lower-level toolkits, DSD has also developed a Visual Composition Environment, or ViCE (see sidebar) to support the collaborative development and execution of complex scientific workflows.

The pyGridWare Toolkit provides a vital set of tools for current Python Grid projects that are transitioning to the new Web service-based Grid architecture. The most recent Grid standards, WSRF and WS-N, are based on industry-standard Web services. A Web service is simply any service that describes its interface in a standard format based on XML and is accessible via standard Web protocols. The use of standard protocols enables the scientific world to leverage the significant corporate investment in Web service infrastructure, and allows multiple interoperable implementations to be developed. pyGridWare is interoperable with the Java and C implementations from Argonne and is mostly compatible with the .Net implementation from the University of Virginia.

In addition to support for developing WSRF applications from scratch, DSD has developed a tool to automatically wrap an existing command-line application to expose it as a WSRF service. This allows a scientist to take an existing application that is run locally and expose it as a Grid service that is accessible over the network.

By allowing existing applications to be easily converted into Grid services, the goal is to leverage the significant investment DOE has made in high performance codes, such as those developed under the SciDAC Integrated Software Infrastructure Centers, while still exposing these applications as Grid services as part of the emerging national middleware infrastructure.

Former DOE Fellow Returns to Berkeley


Jon Wilkening

Jon Wilkening, who earned his Ph.D. in 2002 from UC Berkeley working with CRD Math Group Lead James Sethian, has returned to Berkeley as an assistant professor and collaborator with the Math Group.

Wilkening accepted a DOE Computational Science Graduate Fellowship in 1997 (while declining an NSF fellowship) and was named a Fred A. Howes Scholar in Computational Science in 2003. As a DOE fellow, he worked as a research assistant in the Math Group from 1997 to 2002.

His general research interests include numerical analysis, computational physics, partial differential equations and scientific computing.

Chevessut *(continued from page 1)*

Technique for Key Exchange," which Chevassut co-authored Pierre-Alain Fouque, Pierrick Gaudry, and Pointcheval, will be published in the Proceedings of the Ninth International Workshop on Practice and Theory in Public Key Cryptography (PKC 2006). Chevassut will also present a second paper, along with co-authors Abdalla, Bresson and Pointcheval, on "Password-based Group Key Exchange in a Constant Number of Rounds" at the workshop. The workshop, sponsored by the International Association for Cryptologic Research, will be held April 24-26 at Columbia University in New York. A previous version of the paper can be found at <http://eprint.iacr.org/2005/061>.

Chevassut's third publication, co-authored with Bresson and Pointcheval, is the article "A Security Solution for IEEE 802.11's Ad-hoc Mode: Password-Authentication and Group Diffie-Hellman Key Exchange." The paper will be published early in 2006 in a special issue of the International Journal of Wireless and Mobile Computing that focuses on security of computer network and mobile systems. The article can be found at <http://dsd.lbl.gov/Projects/SecGrpComm/Publications/IJWMC06/ijwmc06.html>.

Chevassut obtained his doctorate in computer science (with a minor in cryptography) for his work on a reliable and secure group communication system at both the Universite Catholique de Louvain in Belgium and Berkeley Lab.